

§ 105–64.107

are reviewed to ensure they are relevant, necessary, accurate, up-to-date, and covered by the appropriate legal or regulatory authority. A listing of GSA Privacy Act Systems can be found at the following link (http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=21567).

§ 105–64.107 What standards of conduct apply to employees with privacy-related responsibilities?

(a) Employees who design, develop, operate, or maintain Privacy Act record systems will protect system security, avoid unauthorized disclosure of information, both verbal and written, and ensure that no system of records is maintained without public notice. All such employees will follow the standards of conduct in 5 CFR part 2635, 5 CFR part 6701, 5 CFR part 735, and 5 CFR part 2634 to protect personal information.

(b) Employees who have access to privacy act records will avoid unauthorized disclosure of personal information, both written and verbal, and ensure they have met privacy training requirements. All such employees will follow GSA orders HCO 9297.1 GSA Data Release Policy, HCO 9297.2A GSA Information Breach Notification Policy, HCO 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII), CIO P 2100.1E CIO P GSA Information Technology (IT) Security Policy, and CIO 2104.1 GSA Information Technology (IT) General Rules of Behavior.

§ 105–64.108 How does GSA safeguard personal information?

(a) System managers will establish administrative, technical, and physical safeguards to ensure the security and confidentiality of records, protect the records against possible threats or hazards, and permit access only to authorized persons. Automated systems will incorporate security controls such as password protection, verification of identity of authorized users, detection of break-in attempts, firewalls, or encryption, as appropriate.

(b) System managers will ensure that employees and contractors who have access to personal information in their

41 CFR Ch. 105 (7–1–13 Edition)

system will have the proper background investigation and meet all privacy training requirements.

§ 105–64.109 How does GSA handle other agencies' records?

In cases where GSA has either permanent or temporary custody of other agencies' records, system managers will coordinate with those agencies on any release of information. Office of Personnel Management (OPM) records that are in GSA's custody are subject to OPM's Privacy Act rules.

§ 105–64.110 When may GSA establish computer matching programs?

(a) System managers will establish computer matching programs or agreements for sharing information with other agencies only with the consent and under the direction of the GSA Data Integrity Board that will be established when and if computer matching programs are used at GSA.

(b) GSA will designate which positions comprise the Data Integrity Board and develop a policy that defines the roles and responsibilities of these positions.

§ 105–64.111 What is GSA's policy on directives that may conflict with this part?

These rules take precedence over any GSA directive that may conflict with the requirements stated here. GSA officials will ensure that no such conflict exists in new or existing directives.

Subpart 105–64.2—Access to Records

§ 105–64.201 How do I get access to my records?

You may request access to your record in person or by writing to the system manager or, in the case of geographically dispersed records, to the office maintaining the records (*see* appendix A to this part). Parents or guardians may obtain access to records of minors or when a court has determined that the individual of record is incompetent.